UNITED STATES DISTRICT COURT

for the

Western District of Washington

In the matter of the Search of Information that is stored at premises controlled by Google, for Investigation of 18 U.S. Code § 641	)	Case No. 3:22-mj-05092

APPLICATION FOR A GEOFENCE SEARCH WARRANT

I, a federal law enforcement officer for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

A Parking Lot as described in Attachment A, incorporated herein by reference.

located in the Northern District of California, there is now concealed *(identify the person or property to be seized):*

See Attachment B, attached hereto and incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S. Code § 641	Theft of government property, it a crime to steal, embezzle, or knowing convert with intent for your own personal gain the property, or to sell, convey, or dispose of any record, voucher, money, or something of value issued by a department of the United States government.

The application is based on the facts set forth in the attached affidavit, which is incorporated herein by reference with all attachments and exhibits.

Pursuant to Fed. R. Crim. P. 41, this warrant is presented by: ☒ by reliable electronic means; or ☐ telephonically recorded.

WARD.NICHOLE.CHRISTINE.1018736990 Digitally signed by WARD.NICHOLE.CHRISTINE.1018736990 Date: 2022.06.02 15:07:18 -07'00'

Applicant's signature

NICHOLE C. WARD, Special Agent

Printed name and title

☐ The foregoing affidavit was sworn before me and signed in my presence, or

☒ The above-named officer provided a sworn statement attesting to the truth or the foregoing affidavit by Telephone.

Date: 6/3/2022

Theresa L. Fricke

Judge's signature

The Honorable Theresa L. Fricke
United States Magistrate Judge

City and state: Tacoma, Washington

Printed name and title

STATE OF WASHINGTON)
) ss
COUNTY OF LEWIS)

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A GEOFENCE SEARCH WARRANT

I, NICHOLE C. WARD, a Special Agent with the United States Army Criminal Investigation Division, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a warrant to search information that is stored at premises controlled by Google, an electronic communication service and remote computing service provider headquartered in Mountain View, California that maintains multiple offices in both Seattle and Kirkland. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a warrant under 18 U.S.C. § 2703(c)(1)(A) to require Google to disclose to the government the information further described in Attachment B, Section I. The government will then review that information and seize the information that is further described in Attachment B, Section II.

2. The purpose of this affidavit is to obtain information identifying any cellular devices that were within one limited geographic area on the date and times when three M4 Rifles were taken from the trunk of a Government vehicle on January 5, 2022.

3. I have been an accredited Federal Special Agent with the USACID since June 11, 2021. I received my law enforcement certification in June 2021 upon completion of the US Army Criminal Investigation Division Special Agent Course through the US Army Military Police School in Ft. Leonard Wood, MO. In 2011, I attended an in-depth 80-hour course in criminal investigations involving Child Abuse and Prevention Techniques as well as attended a follow-on 24-hour course certifying myself as a child forensic interviewer via the Structured Child Interview following the National Institute of

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
253- 428-3800

Child Health and Human Development (NICHD) guidelines. In 2022, I attended an 80-hour Special Victims course, Special Victims Capabilities Course.

4. During my course of employment with the above agency and attendance as a student, I have handled numerous criminal investigations. Those investigations have included numerous deaths, assaults, child assaults, and crimes against persons.

5. I am a "law enforcement officer" of the United States within the meaning of that term contained at 18 U.S.C. § 2510(7) who is empowered by law to conduct investigations of, and to initiate arrests for, various offenses that occur.

6. The information contained in this affidavit is based upon my personal knowledge, observations of other law enforcement personnel and individuals, my review of official police and government reports, and consultation with other personnel involved in the investigation.

7. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter.

8. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S. Code § 641 have been committed by unknown person(s). There is also probable cause to search the information described in Attachment A for evidence of these crimes as further described in Attachment B.

JURISDICTION

9. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

BACKGROUND RELATING TO GOOGLE AND RELEVANT TECHNOLOGY

10. Based on my training and experience, I know that cellular devices, such as mobile telephone(s), are wireless devices that enable their users to send or receive wire and/or electronic communications using the networks provided by cellular service

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
253- 428-3800

providers. Using cellular networks, users of many cellular devices can send and receive communications over the Internet.

11. I also know that many devices, including but not limited to cellular devices, can connect to wireless Internet ("wi-fi") access points if the user enables wi-fi connectivity. These devices can, in such cases, enable their users to send or receive wire and/or electronic communications via the wi-fi network. A tablet such as an iPad is an example of a device that may not have cellular service but that could connect to the Internet via wi-fi. Wi-fi access points, such as those created by a router and offered in places like homes, hotels, airports, and coffee shops, are identified by a service set identifier ("SSID") that functions as the name of the wi-fi network. In general, devices with wi-fi capability routinely scan their environment to determine what wi-fi access points are within range and will display the names of networks within range under the device's wi-fi settings.

12. Based on my training and experience, I also know that many devices, including many cellular and mobile devices, feature Bluetooth functionality. Bluetooth allows for short-range wireless connections between devices, such as between a device such as a cellular phone or tablet and Bluetooth-enabled headphones. Bluetooth uses radio waves to allow the devices to exchange information. When Bluetooth is enabled, a device routinely scans its environment to identify Bluetooth devices, which emit beacons that can be detected by devices within the Bluetooth device's transmission range, to which it might connect.

13. Based on my training and experience, I also know that many cellular devices, such as mobile telephones, include global positioning system ("GPS") technology. Using this technology, the device can determine its precise geographical coordinates. If permitted by the user, this information is often used by apps installed on a device as part of the apps' operation.

14. Based on my training and experience, I know Google is a company that, among other things, offers an operating system ("OS") for mobile devices, including

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
253- 428-3800

cellular phones, known as Android. Nearly every device using the Android operating system has an associated Google account, and users are prompted to add a Google account when they first turn on a new Android device.

15. In addition, based on my training and experience, I know that Google offers numerous apps and online-based services, including messaging and calling (*e.g.,* Gmail, Hangouts, Duo, Voice), navigation (Maps), search engine (Google Search), and file creation, storage, and sharing (*e.g.*, Drive, Keep, Photos, and YouTube). Many of these services are accessible only to users who have signed in to their Google accounts. An individual can obtain a Google account by registering with Google, and the account identifier typically is in the form of a Gmail address (*e.g.*, example@gmail.com). Other services, such as Maps and YouTube, can be used with limited functionality without the user being signed in to a Google account.

16. Based on my training and experience, I also know Google offers an Internet browser known as Chrome that can be used on both computers and mobile devices. A user can sign-in to a Google account while using Chrome, which allows the user's bookmarks, browsing history, and other settings to be uploaded to Google and then synced across the various devices on which the subscriber may use the Chrome browsing software, although Chrome can also be used without signing into a Google account. Chrome is not limited to mobile devices running the Android operating system and can also be installed and used on Apple devices and Windows computers, among others.

17. Based on my training and experience, I know that, in the context of mobile devices, Google's cloud-based services can be accessed either via the device's Internet browser or via apps offered by Google that have been downloaded onto the device. Google apps exist for, and can be downloaded to, devices that do not run the Android operating system, such as Apple devices.

18. According to my training and experience, as well as open-source materials published by Google, I know that Google offers accountholders a service called "Location History," which authorizes Google, when certain prerequisites are satisfied, to

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
253- 428-3800

collect and retain a record of the locations where Google calculated a device to be based on information transmitted to Google by the device. That Location History is stored on Google servers and is associated with the Google account associated with the device. Each account holder may view their Location History and may delete all or part of it at any time.

19. Based on my training and experience, I know that the location information collected by Google and stored within an account's Location History is derived from sources including GPS data and information about the wi-fi access points and Bluetooth beacons within range of the device. Google uses this information to calculate the device's estimated latitude and longitude, which varies in its accuracy depending on the source of the data. Google records the margin of error for its calculation as to the location of a device as a meter radius, referred to by Google as a "maps display radius," for each latitude and longitude point.

20. Based on open-source materials published by Google and my training and experience, I know that Location History is not turned on by default. A Google accountholder must opt-in to Location History and must enable location reporting with respect to each specific device and application on which they use their Google account for that usage to be recorded in Location History. A Google accountholder can also prevent additional Location History records from being created at any time by turning off the Location History setting for their Google account or by disabling location reporting for a particular device or Google application. When Location History is enabled, however, Google collects and retains location data for each device with Location Services enabled, associates it with the relevant Google account, and then uses this information for various purposes, including to tailor search results based on the user's location, to determine the user's location when Google Maps is used, and to provide location-based advertising. As noted above, the Google accountholder also can view and, if desired, delete some or all Location History entries at any time by logging into their

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
253- 428-3800

Google account or by enabling auto-deletion of their Location History records older than a set number of months.

21. Location data, such as the location data in the possession of Google in the form of its users' Location Histories, can assist in a criminal investigation in various ways. As relevant here, I know based on my training and experience that Google can determine, based on location data collected and retained via the use of Google products as described above, devices that were likely in a particular geographic area during a particular time frame and to determine which Google account(s) those devices are associated with. Among other things, this information can indicate that a Google accountholder was near a given location at a time relevant to the criminal investigation by showing that his/her device reported being there.

22. Based on my training and experience, I know that when individuals register with Google for an account, Google asks subscribers to provide certain personal identifying information. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

23. Based on my training and experience, I also know that Google typically retains and can provide certain transactional information about the creation and use of each account on its system. This information can include the date on which the account was created, the length of service, records of login (*i.e.,* session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account.

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
253- 428-3800

In addition, Google often has records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the account.

PROBABLE CAUSE

24. On January 5, 2022, three M4 rifles and one ceremonial bugle were taken from the back of a Government Services Administration vehicle (GSA) at Evergreen Memorial Gardens in Vancouver, Washington. The M4s were used during a funeral Honor Guard. The soldiers left the weapons in the trunk of the GSA as they went inside the funeral home to change out of their uniforms. Upon return to the vehicle, the weapons were gone. The soldiers saw no signs of forced entry. CID contacted the Vancouver Police Department who filed a police report under case number 2022-342.

25. CID personnel conducted a crime scene examination of the honor guard's GSA vehicle located in the parking lot in the vicinity of Building 17, Camp Murray, WA. SA Brandon J. Williams obtained the scene photographs and collected 15 evidence items pertaining to this crime scene examination, to include latent prints. The latent prints were sent to the U.S Army's Criminal Investigation Laboratory (USACIL) for a latent print examination. The examiner positively identified two Honor Guard members as contributors to the latent impressions but could not identify any other possible contributors or "unknown" latent impressions.

26. CID conducted interviews with the soldiers involved, SSG Taha Hakkani, SSG Alvin Proby, and SGT Gregory Conner. All stated they arrived at Evergreen Memorial Gardens around 11:46 a.m., on January 5, 2022. They stated upon arrival, they went inside, spoke with the office staff about the ceremony location, and got changed. All three soldiers said the M2s were left and locked in the trunk of the GSA at this time. The soldiers drove over to the location of the memorial, completed their part of the ceremony, and packed the M4s back into the trunk of the GSA. SGT Conner stated he remembered

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
253- 428-3800

looking at his watch once they got back into the GSA and noted the time to be 12:46 p.m. SGT Conner said they drove back to Evergreen Memorial Gardens and went inside to get changed. He stated the M4s were left unattended and locked in the trunk for no more than 10 minutes while they all went inside. SGT Conner stated once they returned and realized the M4s were missing, he went inside to speak with the building staff. The staff told SGT Conner that a week prior, they had a company truck stolen and had to contact the police on numerous occasions for people sitting in the parking lot "casing the area."

27. All three soldiers stated they did not notice any other vehicles in the parking lot aside from one vehicle parked next to them, unoccupied. The soldiers stated no one approached them either before or after the ceremony. Therefore, the scope of this warrant is unlikely to capture any location data other than the soldiers and suspected person(s).

28. Based on my training and experience, I know that most persons carry a cell phone and/or other computer device with them, either on their person or in their vehicle. I know that nearly every person that I contact has a cell phone that they often use for mapping, communication, or informational applications.

29. Based on the foregoing, I submit that there is probable cause to search information that is currently in the possession of Google and that relates to the devices that reported being within the Target Locations described in Attachment A during the time periods described in Attachment A for evidence of the crime(s) under investigation. The information to be searched includes (1) identifiers of each device; (2) the location(s) reported by each device to Google and the associated timestamp; and (3) basic subscriber information for the Google account(s) associated with each device.

30. The proposed warrant sets forth a multi-step process whereby the government will obtain the information described above. Specifically, as described in Attachment B, Section I:

a. Using Location History data, Google will identify those devices that it calculated were or could have been (based on the associated margin of error for the

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
253- 428-3800

estimated latitude/longitude point) within the Target Locations described in Attachment A during the time periods described in Attachment A. For each device, Google will provide an anonymized identifier, known as a Reverse Location Obfuscation Identifier ("RLOI"), that Google creates and assigns to each device for purposes of responding to this search warrant; Google will also provide each device's location coordinates along with the associated timestamp(s), margin(s) of error for the coordinates (*i.e.,* "maps display radius"), and source(s) from which the location data was derived (*e.g.*, GPS, wi-fi, bluetooth), if available. Google will not, in this step, provide the Google account identifiers (*e.g.,* example@gmail.com) associated with the devices or basic subscriber information for those accounts to the government.

b. The government will identify to Google the devices appearing on the list produced in step 1 for which it seeks the Google account identifier and basic subscriber information. The government may, at its discretion, identify a subset of the devices.

c. Google will then disclose to the government the Google account identifier associated with the devices identified by the government, along with basic subscriber information for those accounts.

31. This process furthers efficiency and privacy by allowing for the possibility that the government, upon reviewing contextual information for all devices identified by Google, may be able to determine that one or more devices associated with a Google account (and the associated basic subscriber information) are likely to be of heightened evidentiary value and warrant further investigation before the records of other accounts in use in the area are disclosed to the government.

32. The proposed warrant would not authorize the disclosure or seizure of any email communications or messages (SMS text or Google chat).

CONCLUSION

33. Based on the foregoing, I request that the Court issue the proposed warrant, pursuant to 18 U.S.C. § 2703(c).

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
253- 428-3800

34. I further request that the Court direct Google to disclose to the government any information described in Section I of Attachment B that is within its possession, custody, or control. Because the warrant will be served on Google, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

WARD.NICHOLE.CHRISTINE.1018736990

Digitally signed by WARD.NICHOLE.CHRISTINE.1018736990
Date: 2022.06.02 14:57:35 -07'00'

NICHOLE C. WARD
Special Agent
US Army Criminal Investigation Division

The above-named agent provided a sworn statement attesting to the truth of the contents of the foregoing affidavit by telephone on the 3rd day of June, 2022.

Theresa L. Fricke

The Honorable Theresa L. Fricke
United States Magistrate Judge

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
253- 428-3800

ATTACHMENT A

Property to Be Searched

This warrant is directed to Google LLC and applies to:

1. Location History data, sourced from information including GPS data and information about visible wi-fi points and Bluetooth beacons transmitted from devices to Google, reflecting devices that Google calculated were or could have been (as indicated by margin of error, *i.e.,* "maps display radius") located within the geographical region bounded by the latitudinal and longitudinal coordinates, dates, and times below ("Initial Search Parameters"); and

2. Identifying information for Google Accounts associated with the responsive Location History data.

//

//

//

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Initial Search Parameters

Search Parameter:

- Date: From January 5, 2022 from 12:50 p.m.–1:05 p.m. (PDT)

- Target Location: Geographical area identified as

  - A polygon defined by the following latitude/longitude coordinates (decimal degrees) connected by straight lines:
    - Point 1: 45.628757, -122.55715
    - Point 2: 45.628659, -122.55717
    - Point 3: 45.628606, -122.55708
    - Point 4: 45.628701, -122.55705

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B

Items to Be Seized

I. Information to be disclosed by Google

The information described in Attachment A, via the following process:

1. Google shall query location history data based on the Initial Search Parameters specified in Attachment A. For each location point recorded within the Initial Search Parameters, and for each location point recorded outside the Initial Search Parameters where the margin of error (*i.e.*, "maps display radius") would permit the device to be located within the Initial Search Parameters, Google shall produce to the government information specifying the corresponding unique device ID, timestamp, location coordinates, display radius, and data source, if available (the "Device List").

2. The government shall review the Device List and identify to Google the devices about which it seeks to obtain Google account identifier and basic subscriber information. The government may, at its discretion, identify a subset of the devices.

3. Google shall disclose to the government identifying information, as defined in 18 U.S.C. § 2703(c)(2), for the Google Accounts associated with each device ID appearing on the Device List about which the government inquires.

This warrant does not authorize the disclosure or seizure of any email communications or messages (SMS text or Google chat).

II. Information to Be Seized

All information described above in Section I that constitutes evidence of violations of 18 U.S. Code § 641 were committed on January 05, 2022 involving an unknown person or persons.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970